LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
Tori Hunthausen,
Chief Deputy Legislative Auditor

Deputy Legislative Auditors:
James Gillett
Angie Grove

MEMORANDUM

TO: Legislative Audit Committee Members

FROM: Dale Stout, Information System Auditor

DATE: April 10, 2007

RE: Information System Audit Follow-up, Datacenter Security (06DP-02)
Montana Department of Transportation

INTRODUCTION

We presented our information system (IS) audit of the Montana Department of Transportation's (MDT) Datacenter Security to the Legislative Audit Committee in December 2005. The report contains two recommendations. The recommendations relate to:

- A lack of processes to identify and manage MDT datacenter environmental threats; and,
- Defining, documenting and implementing an MDT datacenter physical access policy and removing all unnecessary access to the datacenter.

We requested and received information from the Montana Department of Transportation personnel regarding progress toward implementation of our report recommendations. This memorandum summarizes information on the implementation status of each audit recommendation.

BACKGROUND

MDT operates a datacenter that houses approximately $1.2 million of hardware designated to manage data and applications used by MDT to facilitate its business operations. A primary objective of the datacenter is to secure the hardware and information systems where data resides. The security of the datacenter creates the foundation for business continuity by ensuring data and information systems are available by keeping high standards for maintaining the integrity and functionality of the computer environment through the implementation of complete and effective security measures.

Follow-up Discussion

The following sections summarize the report recommendations, and the department's progress towards implementing the recommendations.

Environmental Security Controls

Environmental controls prevent or mitigate potential damage to facilities and interruptions in service caused by unexpected disruptive events (i.e. fire, flood, loss of power, temperature fluctuations, etc). Environmental controls can diminish losses from some interruptions or prevent incidents by detecting potential problems early.

After evaluating the environmental security controls for MDT's datacenter, we discovered MDT could strengthen environmental security controls by conducting an assessment to identify and address threats to the datacenter environment caused by the presence of food and beverages, lack of emergency lighting, location of hardware primary and secondary power supplies and a natural disaster rendering the datacenter physically inaccessible.

Recommendation #1
We recommend the department implement a process to identify and manage environmental threats to the datacenter.

<u>Recommendation Status: **Partially Implemented**</u>

MDT has addressed their datacenter environmental controls as follows:

1. No Food and Beverage – At the time of the audit, MDT did not restrict personnel from bringing food or beverages into the datacenter. Currently a policy has been created to prevent the use of food and beverages in the MDT datacenter. There are also signs posted on each datacenter entrance stating food and beverages are not allowed in the datacenter.

2. Lack of Emergency Lighting – At the time of the audit, MDT did not have lighting in the datacenter in the event of a power outage leaving personnel without the ability to see the equipment to make it operational. Currently, MDT has lighting in the datacenter that will remain on if datacenter power is lost.

3. Location of Power Supplies – At the time of the audit, power supplies and equipment wiring were in the floor. This leaves the wiring and power supplies subject to water accumulation damage. Currently, most power supplies and all equipment wiring has been moved to the ceiling. The remaining power supplies will be moved to the ceiling as datacenter equipment is replaced over the next four years.

4. Business Continuity – If a natural disaster were to strike, the datacenter could be rendered physically inaccessible. If this were to occur, the datacenter and MDT operations would not be able to be restored. Business continuity planning in the form of a disaster recovery plan would allow MDT to be prepared for a natural disaster and could allow the datacenter, and, therefore MDT operations, to continue with the least amount of interruption possible. The risks posed by these natural disasters should also be re-assessed at regular intervals. At the time of the audit, MDT had a draft recovery plan in place for the datacenter, but it did not address recovery if the datacenter were not accessible, contained no natural disaster assessment and no plans to regularly perform the assessment. Currently, MDT has a completed Disaster Recovery Project Charter as well as a plan in place to create a final Disaster Recovery Plan. However, they will not complete the Plan until the completion of legislative and ITSD action regarding legislation for ITSD's new datacenter.

<u>Physical Security Controls</u>

Physical security controls restrict physical access to IT resources by limiting access to the building and rooms where resources are housed. MDT uses an electronic card key access control system; access is limited to individuals who have been assigned a card key.

After evaluating the physical security controls for the MDT datacenter we discovered MDT could strengthen physical security by defining and documenting physical security requirements and procedures specific to the datacenter, and ensuring physical access to the datacenter is limited to only those individuals requiring the access to perform their job duties.

Recommendation #2

We recommend the department:

A. Define, document, and implement a policy to address physical security requirements and procedures specific to the datacenter.
B. Evaluate physical access to the datacenter and remove all unnecessary access.

Recommendation Status: **Implemented**

MDT has addressed their datacenter physical controls as follows:

1. Define, document and implement a policy to address physical datacenter security and procedures - At the time of the audit, the datacenter physical access was controlled by electronic key cards whose use and issuance was governed by policy. The policy did not define datacenter physical access requirements and no documented policy existed to determine who was to authorize datacenter access. MDT re-designed the key card form during our audit but the form did not have a description of how access to the datacenter was to be requested. MDT stated knowledge of the re-designed form would be distributed through their bi-weekly newsletter. Currently, MDT has a datacenter physical access policy in place that defines terms for gaining datacenter physical access, access log reviews, access rights reviews, and what individuals are responsible for granting access. The knowledge of the re-designed physical access form did not occur through the bi-weekly newsletter, but through an agency wide late-breaking news bulletin issued 11/1/2006.

2. Unnecessary access – At the time of the audit we found a terminated employee with datacenter access, 12 individuals with datacenter access but no completed card entry form and datacenter access being provided to individuals not needing that access for their job duties. MDT has reviewed all datacenter access by removing all access from the datacenter and only assigning it back to those that need it to perform their job duties; this resulted in reducing the number of individuals with datacenter access privileges from 25 to 17.